Remarks

Claims 1-5, 8-9, 11-13, 18-111 are currently pending in this application. Claims 6-7, 10, and 14-17 have been cancelled. Claims 1, 37, 46, 48, 61, 64, 67, 74 and 91 have been amended.

Pursuant to the discussion in the interview with the Examiner, claims 1 and 37 have been amended to clarify that the configuration data is for configuring the integrated circuit. Claims 61, 64, 67 and 74 have been amended to clarify that the configuration data is for configuring the field programmable gate array. Claims 46 and 48 have been amended to clarify that the field programmable gate array is an integrated circuit. Claim 37 has also been amended to provide a consistent antecedent basis for the "first security key". Claim 91 has been amended to provide proper antecedent basis for "non-volatile register".

1. Claims 30 and 42 were amended in the previous response to overcome the section 112 rejections.

The Examiner has maintained the prior rejections of claims 30, and 42 under 35 USC 112 as being indefinite. Claim 30 was amended in the previous response to more distinctly claim the subject matter of the invention of claim 30. Claim 42 was also amended in the previous response to replace "the configured user logic" with "the user programmed circuitry", to provide proper antecedent basis for this limitation. It appears that these rejections were inadvertently carried over from the prior office action, and thus these rejections should be withdrawn as moot.

2. The limitation "about" is not indefinite in claims 54 and 55, because broadening claim limitations such as "about" do not impart invalidity to the claims, as confirmed by the Federal Circuit.

The Examiner has also rejected claims 54 and 55 under 35 USC 112 as being indefinite, because these claims include the limitation "about". The limitation "about" as used in claims 54 and 55 is a term of degree, used to provide a clear and definite, but flexible, range such that one skilled in the art would understand what was claimed. See MPEP

2173.05(b)(A). This usage is supported in the specification, for example at paragraph [0024] and at paragraph [0118]. Furthermore, the Federal Circuit has recognized that the term "about" does not render a patent claim invalid, where those skilled in the art would understand what was claimed, as is the case here. See Andrew Corp. v. Gabriel Electronics, Inc. 847 F.2d 819, 821-22 (Fed. Cir. 1988). Thus Applicant's use of the limitation "about" in claims 54 and 55 do not render those claims indefinite, and thus Applicant respectfully requests that the rejections be withdrawn.

3. Claims 1-36 are not anticipated or rendered obvious, because the Garnett reference teaches encrypting the bitstream outside the FPGA.

Independent claim 1 currently stands rejected over US Patent No. 6,356,637 to Garnett (hereinafter "Garnett"). Claim 1 has been amended to recite, *inter alia*, a method of operating an integrated circuit comprising "inputting a stream of data comprising unencrypted configuration data to the integrated circuit" and "encrypting the unencrypted configuration data using a security circuit contained within the integrated circuit and a security key stored in the integrated circuit" (emphasis added). Thus the amended claim 1 clearly recites that the security circuit is contained within the integrated circuit.

In contrast, Garnett describes a straightforward approach wherein a bitstream (i.e. configuration data) is created according to standard methods, by an application designer who wishes to configure the FPGA. (Col 6, lines 8-11). The designer then encrypts the configuration data, outside the FPGA, using conventional Computer-Aided Design (CAD) tools. (Col. 6, lines 11-15). The CAD tool used to encrypt the data may be either a software or hardware based tool, and may be supplied by the designer or the FPGA manufacturer. In any event, this design tool is external to the FPGA. (Col. 4, lines 10-21). This already-encrypted configuration data is then loaded into configuration data storage, for later use by the FPGA. (Col. 6, lines 15-19). When the FPGA later loads the encrypted configuration data from the configuration data storage, the FPGA decrypts the configuration data and uses the decrypted data to configure the FPGA. (Col. 6, lines 50-57). By teaching the use of conventional CAD tools to perform the encryption, outside of

the FPGA, Garnett expressly teaches contrary to and away from the method of claim 1, which claims "encrypting the unencrypted configuration data using a security circuit contained within the integrated circuit and a security key stored in the integrated circuit."

By performing the encryption using a security circuit contained within the integrated circuit, the method of claim 1 advantageously helps keep the encryption key secure, because the encryption key does not have to be maintained on a separate computer used to host the CAD tools, as required by Garnett. Furthermore, the encryption key can be automatically matched to a decryption key when using the method of claim 1, whereas with the methods disclosed by Garnett, the design fabricator would have to manually ensure that the encryption and decryption keys match each other (i.e. that the decryption key is effective to decrypt a bitstream which was encrypted by the encryption key, and vice versa).

Garnett does not teach inputting unencrypted configuration data to the integrated circuit and encrypting the unencrypted configuration data on the integrated circuit. Garnett teaches the conventional method of loading configuration data into an FPGA, wherein the configuration data is encrypted by the application designer outside of the FPGA, using a hardware or software-based design tool. Therefore, independent claim 1, as well as dependent claims 2-36 that depend from independent claim 1, are neither anticipated by Garnett nor obvious over Garnett and the other references cited by the Examiner.

4. Claims 37- 45 are not rendered obvious by Garnett and Hair because Garnett teaches encrypting the bitstream outside of the FPGA.

Independent claim 37 currently stands rejected over Garnett in view of US Patent No. 6,615,349 to Hair (hereinafter "Hair"). Claim 37 recites, *inter alia*, a method of operating an integrated circuit comprising "encrypting the unencrypted configuration data using a second security key and a fixed security circuit contained within the integrated circuit" (emphasis added). Thus the amended claim 37 clearly recites that the security circuit is contained within the integrated circuit.

In contrast, as discussed above, Garnett describes a straightforward approach wherein a bitstream (i.e. configuration data) is encrypted, outside the FPGA, using conventional Computer-Aided Design (CAD) tools. (Col. 6, lines 11-15). This encrypted configuration data is then loaded into configuration data storage, for later use by the FPGA. (Col. 6, lines 15-19). When the FPGA later loads the encrypted configuration data from the configuration data storage, the FPGA decrypts the configuration data and uses the decrypted data to configure the FPGA. (Col. 6, lines 50-57). By teaching the use of conventional CAD tools to perform the encryption, outside of the FPGA, Garnett expressly teaches contrary to and away from the method of claim 37, which claims "encrypting the unencrypted configuration data using a second security key and a fixed security circuit of the integrated circuit."

5. Claims 37- 45 are not rendered obvious by Garnett and Hair because the non-analogous Hair reference teaches methods that are unworkably complex for FPGA technology.

The Hair reference teaches that encrypted computer files which are transmitted across a computer network to a receiving computer may be encrypted again by an encrypting file system of the personal computer before being stored locally on a computer storage device. (Col. 5, lines 27-33). Hair teaches using a complex data communications encryption algorithm, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS) to encrypt the communicated data. (Col. 2, lines 25-30) Similarly, on the computer, complex algorithms such as Layer 2 Tunneling Protocol (L2TP), IP Security Protocol (IPSEC), and Windows 2000 Encrypting File System (EFS) are taught by Hair. (Col. 3, lines 33-65). These algorithms require powerful personal computers, with effectively unlimited program and data memory, as well as a lot of computing power, in order to implement.

Hair does not teach the use of "a second security key and a fixed security circuit contained within the integrated circuit" to perform any encryption or decryption functions, as claimed in claim 37. Hair implements its complex security algorithms using

complex computer software programs and operating system programs, (Col. 8, lines 58-67), which would have been impossible to implement on an FPGA as of the filing date of the application. FPGA configuration circuits as of the filing date of this application were typically implemented as simple groups of hardware state machines, which lacked the immense resources needed to implement the methods taught by Hair. For example, the reference Xilinx XC4000XLA (hereinafter "Xilinx XC4000") cited by the Examiner teaches that top-of-the-line FPGAs as of October 1999 contained a maximum memory of about 270,000 bits (i.e. about 32K), and a maximum number of logic gates of only 250,000. The typical circuits configured into this FPGA would not be able to process the complex security algorithms taught by Hair. Thus Garnett, even in combination with Hair, fails to anticipate or render obvious the inventions of claim 37 or its dependent claims 38-45.

6. Claims 46-77 are neither anticipated nor rendered obvious, because the claims recite a novel combination of on-chip FPGA configuration data encryption and/or decryption, volatile key storage memory and a battery backup, not taught by Garnett or the non-analogous Wong reference.

Claims 46-77 stand rejected under Garnett in view of US Patent 5,596,512 to Wong (hereinafter "Wong") and several other references. None of the references cited by the Examiner, either alone or when properly combined, teach the inventions of claims 46-77. There are many differences between the references cited by the Examiner and claims 46-77, but one difference in particular is that each of the claims 46-77 recite either a "battery-backed on-chip memory", an "on-chip battery-backed register", an FPGA "to be coupled to an external backup battery", an FPGA "connectable to an external backup battery" or a method of using an FPGA that is "connectable to an external backup battery" or an FPGA that has "a battery connected to the second positive supply input pin" of the FPGA. All of these are for the purpose of connecting a backup battery to an element of the FPGA which stores a cryptographic or security key.

Thus, claims 46-77 are directed to the novel and non-obvious combination of providing on-chip encryption and/or decryption for the FPGA configuration data along with a smaller volatile memory for the key storage element, coupled to a battery backup. This advantageously reduces power consumption relative to conventional systems which provide a battery backup to the entire configuration memory.

7. In contrast, the Examiner's primary reference cited against the claims in the instant application, US Patent No. 6,356,637 to Garnett (hereinafter "Garnett"), describes using a "relatively large" non-volatile memory to store the decryption key. See Garnett, col. 2, lines 26-31. Garnett also teaches performing the encryption off-chip, not on-chip.

Garnett teaches a straightforward approach wherein a bitstream (i.e. configuration data) is created according to standard methods, by an application designer who wishes to configure the FPGA. (Col 6, lines 8-11). The designer then encrypts the configuration data, outside the FPGA, using conventional Computer-Aided Design (CAD) tools. (Col. 6, lines 11-15). This encrypted configuration data is then loaded into configuration data storage, for later use by the FPGA. (Col. 6, lines 15-19). When the FPGA later loads the encrypted configuration data from the configuration data storage, the FPGA decrypts the configuration data and uses the decrypted data to configure the FPGA. (Col. 6, lines 50-57). The FPGA uses a decryption key stored in a decryption key storage 6, which is a non-volatile memory on the FPGA. (Col. 5, lines 19-32). Since the decryption key storage 6 is non-volatile memory, there is no need for the FPGA discussed in Garnett to have any kind of battery backup, and Garnett does not anywhere mention the use of a battery backup. Garnett does not provide a separate power source to one portion of a microchip. Garnett does not teach any kind of a solution to the problems solved by the inventions of claims 46-77. In fact, by teaching the use of non-volatile memory for the decryption key storage 6, Garnett teaches away from the idea of using a key storage that needs to be connected to a battery backup, or from using an on-chip memory for storing a cryptographic key, wherein the on-chip memory is connectable to an external backup

battery, as claimed in claims 46-77. Thus Garnett does not anticipate nor render obvious claims 46-77.

The Examiner also cited Wong against claims 46-77 of the instant application, for the contention that it would have been obvious to combine Garnett and Wong to teach an FPGA with a battery backed memory for security key storage. Wong is a patent directed to a completely non-analogous art, namely refrigeration system controllers for big-rig trucks. See Wong, col. 2, lines 50-65. Controllers for controlling mechanical parts installed on big-rig trucks have nothing to do with microchips such as FPGAs, nor with cryptography used on FPGAs. It would not have been obvious for one skilled in the art of FPGA design to look to the non-analogous art of big-rig truck systems design. For example, FPGA designers are looking to keep component size as small as possible, whereas big-rig truck system designers are not so constrained. It is a lot easier to use separate power supplies for different components on a large board-level design such as a controller for big rig refrigeration systems, than it would be for a much smaller integrated circuit such as an FPGA. There are no significant issues with segregating the components on a large board-level design into backed-up and a non-backed-up groups such that the non-backed-up group does not siphon off power from the battery when the main power is off. This segregation issue is much more significant on single small microchips such as FPGAs. Tellingly, Garnett, which is a reference that discusses FPGAs, discusses many different types of non-volatile memory (e.g. EEPROMs, flash memory, fusible link PROMs, UV-EPROMs, OTPROMs, ferroelectric cells, and laser programmable fuses), but never mentions using any form of volatile memory for storage of the security key, nor any form of separate power supply or battery for part of the microchip, such as the security key register.

8. Claims 78-90, 96-111, rejected as corresponding to elements of rejected claims 1-45, 54-55, are neither anticipated nor obvious, for the same reasons that claims 1-45, 54-55 are neither anticipated nor obvious.

Claims 78-90, 96-111 currently stand rejected over Garnett as modified for claims 46-53, in further view of Pedram. The Examiner rejects claims 78-90, 96-111 as corresponding to rejected claims 1-45, 54-55. As explained in detail above, the cited references do not anticipate claims 1-45, 54-55, and thus also do not anticipate claims 78-90, 96-111. For example, claims 78-90 relate to securely configuring an FPGA by, *inter alia*, "determining, based on the header information [found in the bitstream], a security processing operation to apply to the bitstream". None of the references cited by the Examiner, either alone or in combination, teach or suggest the inventions of claims 78-90. As recognized by the Examiner, the Garnett reference fails to teach the use of headers in FPGA bitstreams for the purpose of encryption or decryption of the bitstreams. In rejecting other claims of the present application, the Examiner contends that it would have been obvious to combine Garnett with up to five other references, including a paper by Chambers, et al, titled "TCP/IP Security" (hereinafter "TCP/IP Security"), to reach the idea of using headers in FPGA bitstreams for the purpose of encryption or decryption of the bitstreams.

TCP/IP Security is a publication regarding complex security protocols, such as IPSEC, SSL, and TSL, which are layered on top of a complex communications protocol (TCP/IP). These security protocols require a very large number of bits to implement, and are only practical in environments such as Internet communications where bandwidth and storage costs are relatively low. TCP/IP Security has nothing to do with FPGA circuits or communications with FPGAs. In the year 2000, when this application was filed, FPGA configuration circuits were simple, very small pieces of hardware designed to load a sequence of bits into a RAM configuration memory and to use as little area as possible within the FPGA. Area on an FPGA was in very short supply, and using a highly complex protocol such as the security protocols discussed in TCP/IP Security to implement security would have been impossibly expensive in terms of storage and bandwidth. Taking a highly complex and large security protocol such as those discussed in TCP/IP Security, which were normally implemented in software, on top of the TCP/IP protocol, on complex communications equipment such as routers, personal computers, and mainframes, and using such a security protocol on a small, simple FPGA

configuration circuit would not have been obvious as of the filing of this application in 2000. One skilled in the art of FPGA circuit design would not have been motivated to look to the non-analogous art of computer-to-computer communications security protocols to modify the teachings of Garnett. It is this application which provides the motivation to implement headers for indicating the encrypted/non-encrypted status of a bitstream in FPGAs, and as such it is improper hindsight to combine the cited references as the Examiner has done.

9. Claims 91-95 are neither anticipated nor obvious, because Garnett fails to teach the use of error-correction circuits, the non-analogous Schneier reference teaches error detection, not correction, and the non-analogous Schneier reference teaches methods from computer to computer communications that are unworkably complex for FPGA technology.

Claims 91-95 currently stand rejected over a combination of Garnett and numerous other references, including US 6233717 to Choi. Claims 91-95 as amended relate to using an error-correcting code circuit with an unreliable non-volatile key register. None of the references cited by the Examiner anticipate or render obvious the inventions of claims 91-95. The Examiner recognizes that the cited references, other than Choi, do not teach error correction. Choi does teach error correction in memory arrays. However, Choi does not teach " wherein the unreliable memory cells are fabricated using memory cell technology compatible with standard CMOS processing". A novel advantage to the circuit of claims 91-95 is that such circuits may be constructed using standard CMOS processing, without requiring any additional manufacturing options normally used to fabricate non-volatile memories. These additional processes, which are conventionally used in CMOS processing to create non-volatile memory and result in creation of reliable memory cells, have an adverse affect on the FPGA speed and gate density. Thus the additionally processed FPGAs are slower and contain fewer gates. The FPGA of claims 91-95 avoids this disadvantage by intentionally using a process which creates smaller, faster, but unreliable memory cells, and uses ECC techniques to compensate for any errors created by the unreliable memory cells. There is no motivation provided by Choi,

Garnett or any of the other references to intentionally use a lower quality manufacturing process to create the memory cells for the non-volatile register that stores the security key, when conventional methods include the higher quality manufacturing processes which create reliable memories. It would not be obvious to use a process which is known to give unreliable memories and then correct those results with ECC when there are available process options which produce reliable memories. Thus claims 91-95 are not obvious over Garnett, Choi or any of the other cited references, and the rejections of claims 91-95 should be withdrawn.

Conclusion

Prompt and favorable action on the merits of the claims is earnestly solicited. Should the Examiner have any questions or comments, the undersigned can be reached at (949) 567-6700.

The Commissioner is authorized to charge any fee which may be required in connection with this Amendment to deposit account No. 15-0665.

Respectfully submitted,
ORRICK, HERRINGTON & SUTCLIFFE LLP

Dated: November 17, 2005

By: Donald Daybell
Donald Daybell
Reg. No. 50,877

Orrick, Herrington & Sutcliffe LLP
4 Park Plaza, Suite 1600
Irvine, CA 92614-2558
Tel. 949-567-6700
Fax: 949-567-6710